REMARKS

In this Amendment, Applicant has amended Claims 1 – 4. Claims 1 – 4 have been amended to overcome the rejections and further specify the embodiments of the present invention. The specification has been amended at various paragraphs to rephrase certain expressions and correct clerical errors. The amendment is editorial in nature. It is respectfully submitted that no new matter has been introduced by the amended claims and specification. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

CLAIM OBJECTION:

Claim 1 has been objected as containing informalities.

By this amendment, Claim 1 has been amended to delete one "on" in line 5. Therefore, the objection to Claim 1 has been overcome and withdrawal of objection is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 112 SECOND PARAPGRAPH:

Claims 1 – 4 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is respectfully submitted that the rejections have been overcome by this amendment. More specifically, in Claim 1, "alternate converting said subblocks" has been amended to "converting in turn said subblocks"; "dual-locus operation" has been amended to "two-place operation". In addition, Claim 1 has been amended to specify that the feature of "transforming the subkey with a data-dependent operation that depends on the j-th subblock prior to performing the two-place operation on the i-th subblock and subkey, where i≠j."

Furthermore, Claims 2 – 4 have been amended to clearly define the embodiments of the present invention. In particular, Claim 2 has been amended to define that "data dependent permuting subkey bits is used as data-dependent operation that depends on the j-th subblock." Claim 3 has been amended to define that "data-dependent rotation of subkey bits is used as data-dependent operation that depends on the j-th subblock." Claim 4 has been amended to define that "a data-dependent substitution operation performed on a subkey is used as data-dependent operation that depends on the j-th subblock."

Therefore, the rejection under 35 U.S.C. § 112, second paragraph, has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 112, second paragraph, is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 102:

Claim 1 has been rejected under 35 U.S.C. § 102 (e) as allegedly being anticipated by Den Boer et al. (US 6,298,136), hereinafter Den Boer.

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. The embodiment of the present invention as defined in Claim 1 is different from the disclosure in Den Boer. Claim 1 has been amended to further specify the embodiments of the present invention and include "transforming the subkey with a data-dependent operation that depends on the j-th subblock prior to performing the two-place operation on the i-th subblock and subkey, where i≠j." Therefore, the embodiments of the present invention include the feature of converting subkeys using an operation dependent on data subblocks being converted. Such feature is not disclosed in Den Boer.

In Den Boer, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Den Boer. To the contrary, the embodiments of the present invention as claimed indicate that, at a preset conversion step, the value of subkeys is different in encrypting different data blocks. This is ensured by the fact that the subkeys are converted using the operation that depends upon subblocks of the data block being converted.

Therefore, the newly presented claim is not anticipated by Den Boer and the rejection under 35 U.S.C. § 102 (e) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (e) is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103:

Claims 2 – 4 have been rejected under 35 U.S.C. § 103 as allegedly being unpatentable over by Den Boer, in view of Coppersmith et al. (US 6,192,129), hereinafter Coppersmith.

Applicant traverses the rejection and respectfully submits that the embodiments of present-claimed invention are not obvious over Den Boer, in view of Coppersmith. At first, Claims 2 – 4 also include the feature of "transforming the subkey with a data-dependent operation that depends on the j-th subblock prior to performing the two-place operation on the i-th subblock and subkey, where i≠j" by their dependency on Claim 1. As stated above, Den Boer does not disclose the invention as amended. Similarly, Coppersmith also fails to teach or suggest the embodiments of the present invention as defined in Claims 2 – 4. In Coppersmith, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Coppersmith. In addition, as admitted by the Examiner, Den Boer does not expressly disclose either an operation of permuting subkey bits or a substitute operation performed on a subkey as being the conversion operation step. Therefore, there is no motivation to combine Den Boer and Coppersmith. Even if they are combined, Den Boer and Coppersmith will not render the present claimed invention obvious. One of ordinary skill in the art would not discern the present invention as claimed at the time of its invention.

Therefore, the newly presented claims are not anticipated by Den Boer and Coppersmith and the rejection under 35 U.S.C. § 103 has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103 is respectfully requested.

Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

By
John C. Holman
Registration No. 22,769

Date: August 13, 2004
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0